LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för kalenderåret 2005

KRYPTOTEKNIK EDI051

Cryptography

Antal poäng: 5. **Betygskala:** TH. **Valfri för:** C4, D4, E4, F4, Pi4XSi, RH4. **Kursansvarig:** Professor Thomas Johansson, Inst f informationsteknologi. **Prestationsbedömning:** Godkända projekt är krav för att få tentera. Tentamen (5 tim) är skriftlig och av problemlösningstyp. **Hemsida:** http://www.it.lth.se/courses/cryptology.

Mål
Syftet med kursen är att ge en orientering om klassiska kryptosystem samt att ge ingående kunskaper om moderna kryptosystem.

Innehåll
Klassiska kryptosystem: Inledning och grundläggande begrepp. Caesarkrypto, enkel substitution, polyalfabetssystem (Vigenére, Kasiskis forceringsmetod, Vernam), bigramsubstitution, transposition.
Shannons teori för sekretess: Nyckelentropier och meddelanden, redundans och entydighetslängd, perfekt sekretess.
Kryptomaskiner: Hagelins M-209 maskin, rotormaskiner (Enigma).
Skiftregister och strömchiffer: Något om ändliga kroppar, linjärt återkopplade skiftregister och skiftregistersekvenser, perioder och cykelkarakteristiker, skiftregistersyntes, olinjära kombinationer av skiftregistersekvenser, skiftregisterfiltrering.
Blockchiffer: Data Encryption Standard: Historik, konstruktionsfilosofi.
Öppen-nyckel-distribution: Logaritmproblemet, Pohlig-Hellman-systemet.
Öppen-nyckel-kryptosystem: Något om talteori, RSA-systemet, Diffie-Hellman nyckelutbyte.
Simmons teori för autenticering: Imitation och substitution, Simmons gräns. Secret sharing.
Secret sharing: Shamirs tröskelschema, generell secret sharing.
Projekt: 1. Studium av skiftregister, 2. Learning about DES. 3. Faktoriseringsalgoritmer. 4. Korrelationsattacker.

Litteratur
Kompendium i kryptoteknik, 2004, utges av institutionen (Johannesson R: Något om kryptering)